別紙 3

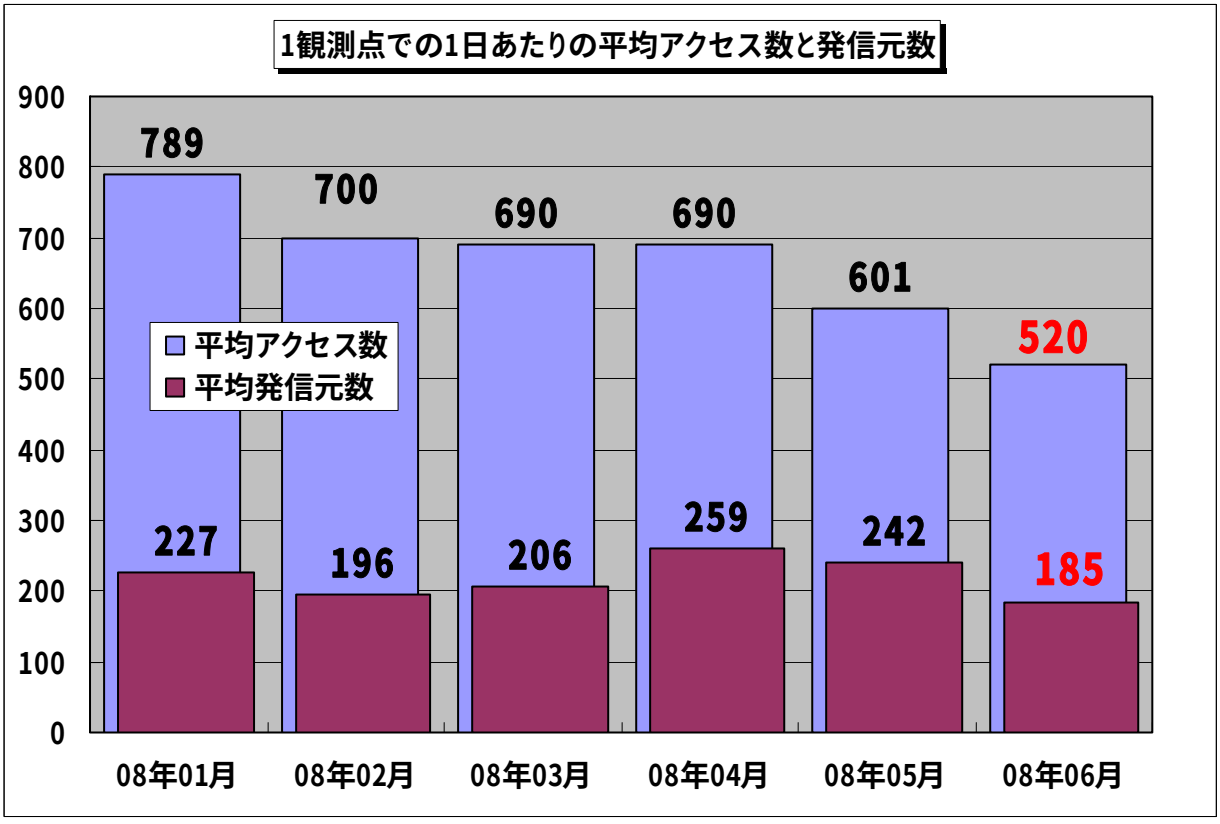
インターネット定点観測(TALOT2)での観測状況について

1．一般のインターネット利用者の皆さんへ

インターネット定点観測(TALOT2)によると、2008 年 6 月の期待しない（一方的な）アクセスの総数は 10 観測点で **156,012 件**、総発信元数(※)は **55,589 箇所**ありました。1 観測点で見ると、1 日あたり **185** の発信元から **520 件**のアクセスがあったことになります。

総発信元数（※）：TALOT2 にアクセスしてきた発信元の総数。なお、同一発信元から同一観測日・観測点・ポートにアクセスがあった場合は 1 つの発信元としてカウント。

TALOT2 での 1 観測点の環境は、インターネットを利用される一般的な接続環境と同一なので、インターネットを利用される皆さんの環境へも同じくらいの一方的なアクセスがあると考えられます。言い換えれば、**あなたのコンピュータは、毎日、平均して、185 人の見知らぬ人(発信元)から、発信元一人当たり約 3 件の不正と思われるアクセスを受けている**と言うことになります。



【図 1.1　1 観測点での 1 日あたりの期待しない(一方的な)アクセス数および発信元数】

2008 年 1 月～2008 年 6 月までの各月の 1 観測点での 1 日あたりの平均アクセス数および、それらのアクセスの平均発信元数を図 1.1 に示します。この図を見ると、6 月の期待しない（一方的な）アクセスは 5 月と比べて減少しており、過去 6 ヶ月間を通してみても、徐々に減少傾向を示していると言えます。

2．6 月のアクセスの状況

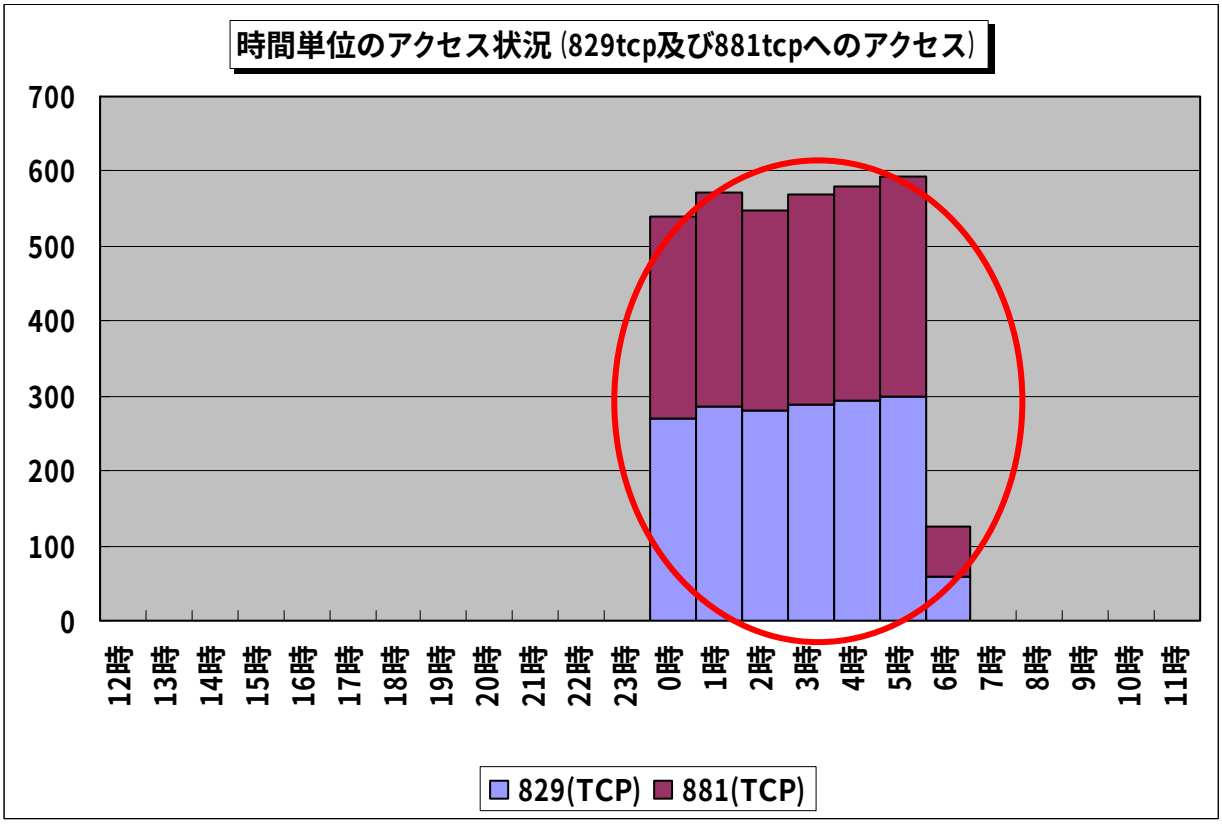
2008 年 6 月のアクセス状況は、5 月と比べて減少しました。これは主に Windows Messenger サービスを悪用してポップアップメッセージを送信するアクセスである 1026/udp、1027/udp および 1028/udp などへのアクセスが減少したためです。その他のポートへのアクセスについては特に大きな変化はありませんでした。

2.1．DoS 攻撃（SYN Flood 攻撃）(*1)の影響と思われるアクセス

6 月の後半に香港方面の通信事業者を狙った DoS 攻撃（SYN Flood 攻撃）の影響と思われるアクセスが 2 箇所の観測点で確認されています。これらのアクセスは宛先ポート 829/tcp 及び 881/tcp（発信ポートは 80）への SYN+ACK パケットでした。

TALOT2 で使用しているアドレスが、攻撃者が発信元詐称に利用したアドレスと一致した為に、標的となった企業からの SYN+ACK パケットが大量に届いたということです。その時の時間単位のアクセス状況を図 2.1.1 に示します。

※このアクセスは直接的な攻撃を狙ったアクセスではなく統計情報にそぐわない為、集計からは除外しています。



【図 2.1.1 香港方面への SYN Flood 攻撃のバックスキャッタ (*3)】

TALOT2 が観測点として使用しているアドレスは、不定期に変更しています。今回取得した 10 箇所のアドレスのうち、2 箇所もこの攻撃に利用されていたということは、他にも利用されていたアドレスが多数あると推測されます。

このように本人が攻撃対象として狙われていなくても、不正なアクセスを受信することがあるので、外部からの不要なポートがファイアウォールでフィルタリングされているか確認することをお勧めします。

(*1):DoS 攻撃（SYN Flood 攻撃）

「サービス妨害攻撃」Denial of Service の略からＤｏＳ攻撃と呼ばれ、標的マシンにおけるサービス機能を停止または低下させる攻撃のこと。このＤｏＳ攻撃の1つに、標的マシンに「過負荷を与える攻撃」として SYN Flood 攻撃があります。これは、標的マシンに対して発信元アドレスを詐称した SYN パケット(3 ウェイ・ハンドシェーク(*2)での接続確立の最初に送られる

パケット)を大量に送りつけ、確立途中状態の接続を大量作成するものです。

(*2):3 ウェイ・ハンドシェーク

TCP で通信を行う際に、最初に行われる通信確立のための手順を、3 ウェイ・ハンドシェークと言います。この手順により、通信を行う相手同士が通信の準備ができたことを確認できるわけです。

以下に A と B の通信確立の手順を示します。

①A から B へ SYN パケットの送信

②B から A へ ACK+SYN パケットの送信

③A から B へ ACK パケットの送信

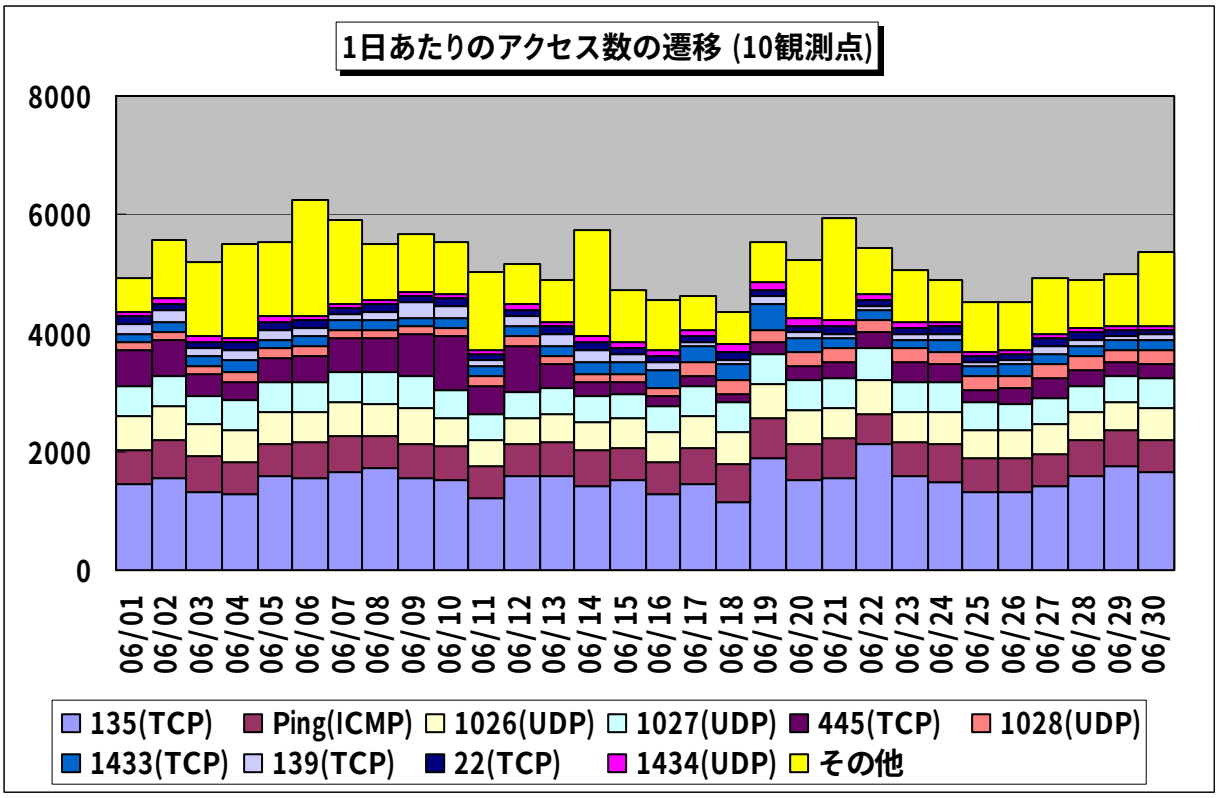
これで、AB 双方の通信が確立されます。

(*3):バックスキャッタ

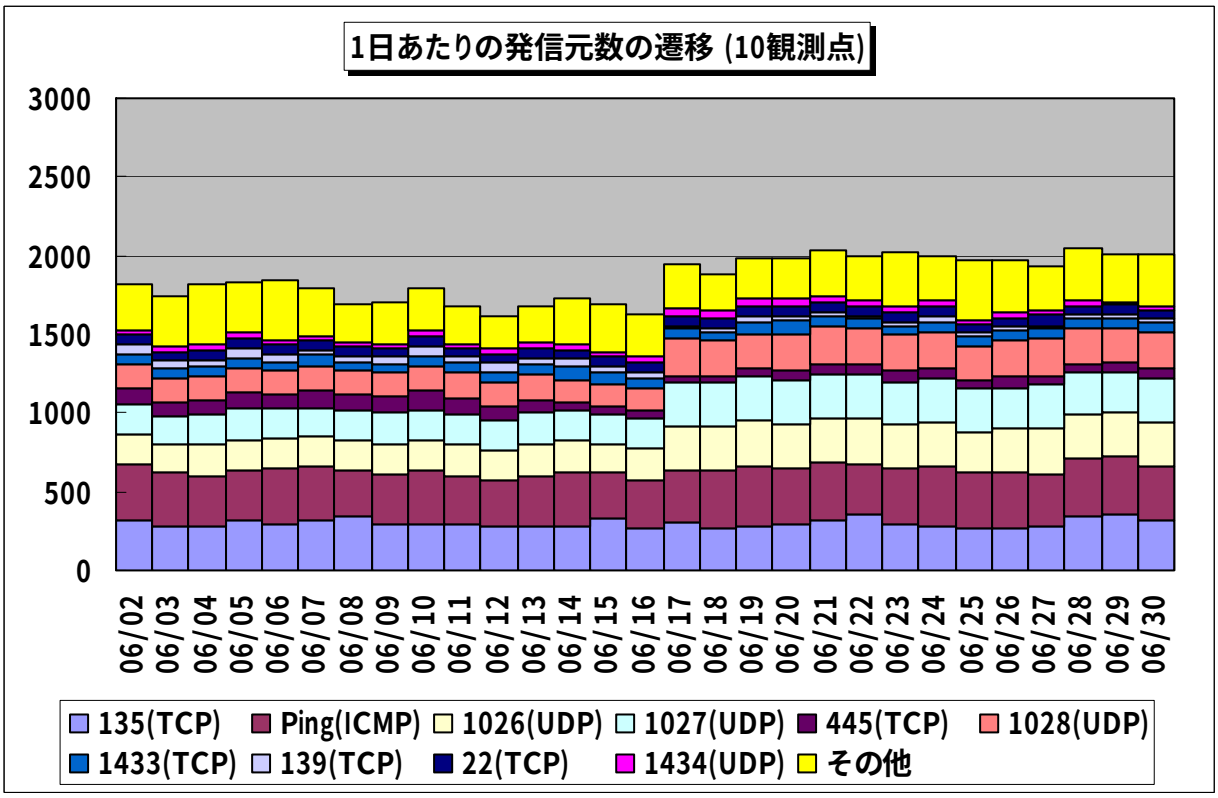
DoS 攻撃（SYN Flood 攻撃）において攻撃者が詐称した発信元アドレスに、標的マシンから大量の SYN+ACK パケットが返信されてくることです。

2.2 2008 年 6 月の一方的なアクセス状況

2008 年 6 月の一方的なアクセス状況（アクセス数）の遷移を図 2.2.1 に、一方的なアクセス状況（発信元数）の遷移を図 2.2.2 に示します。



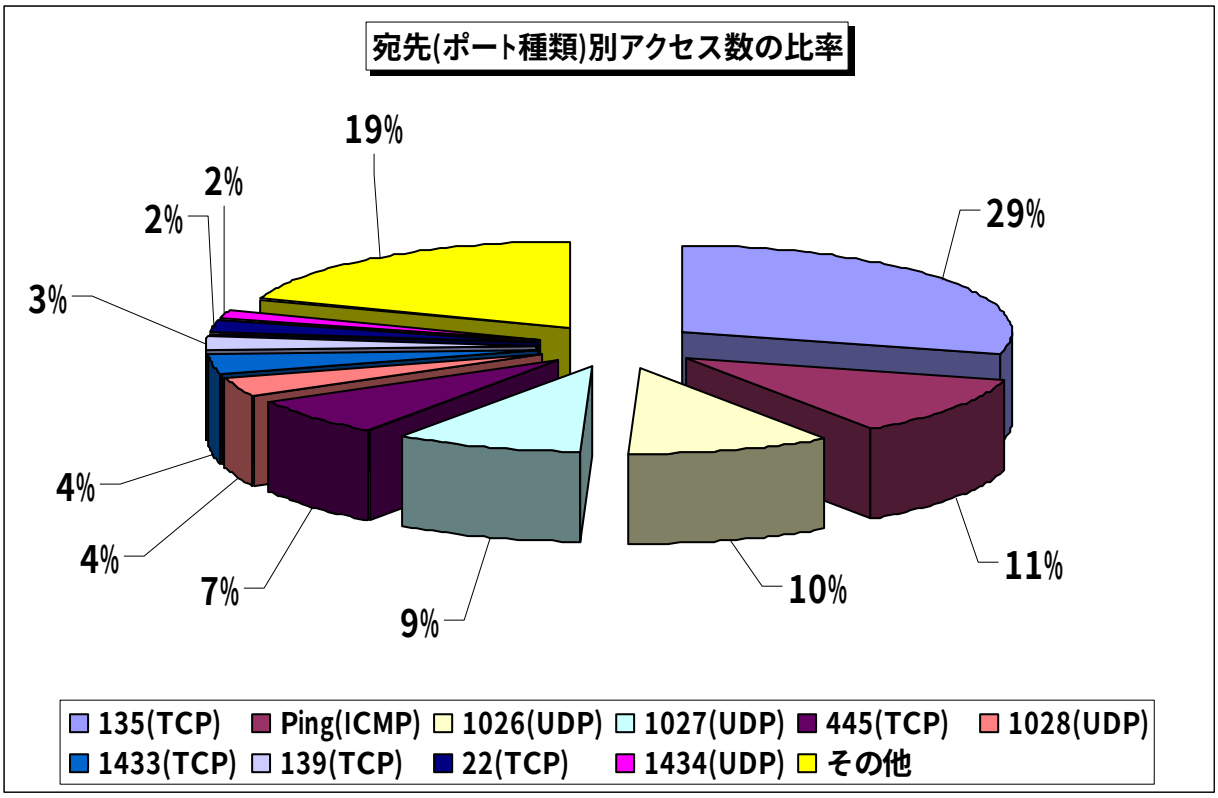
【図 2.2.1 2008 年 6 月の一方的なアクセス状況(アクセス数)】



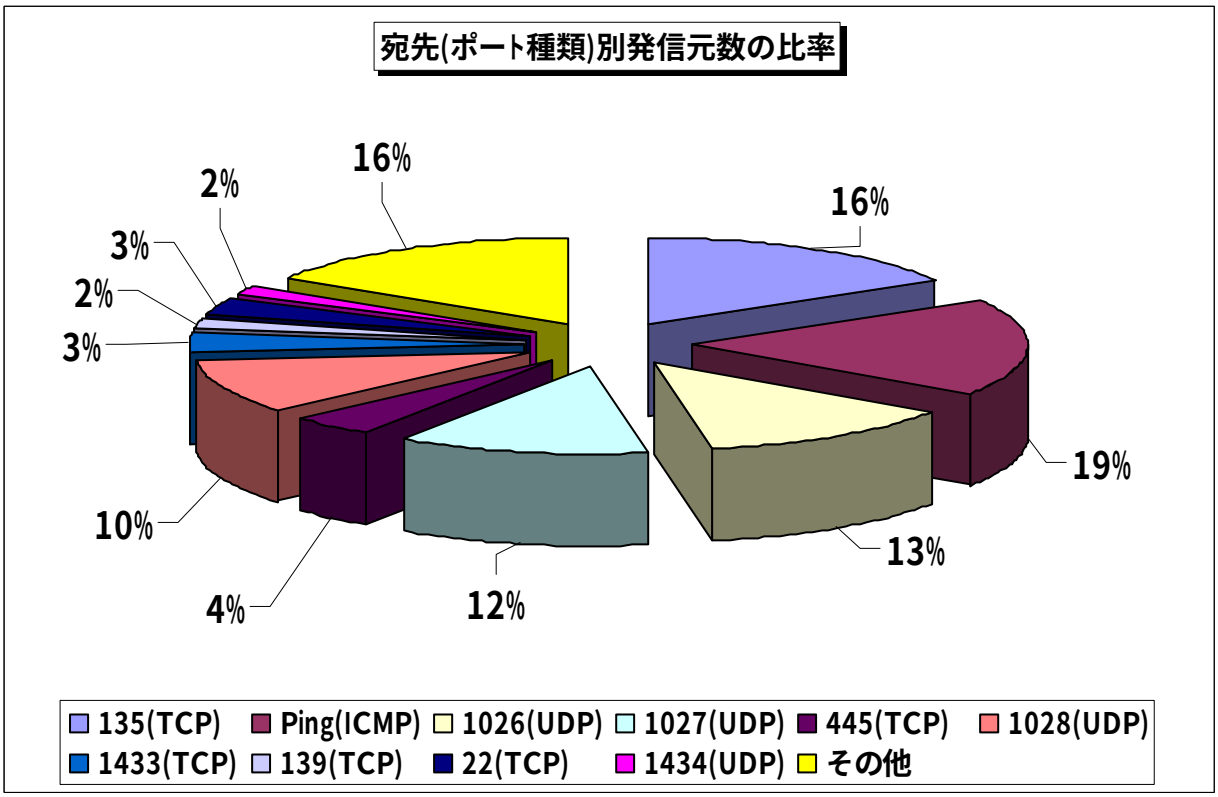
【図 2.2.2 2008 年 6 月の一方的なアクセス状況(発信元数)】

2.3 2008 年 6 月の宛先(ポート種類)別の比率

2008 年 6 月の一方的なアクセスの宛先(ポート種類)別アクセス数の比率を図 2.3.1 に、宛先(ポート種類)別発信元数の比率を図 2.3.2 に示します。



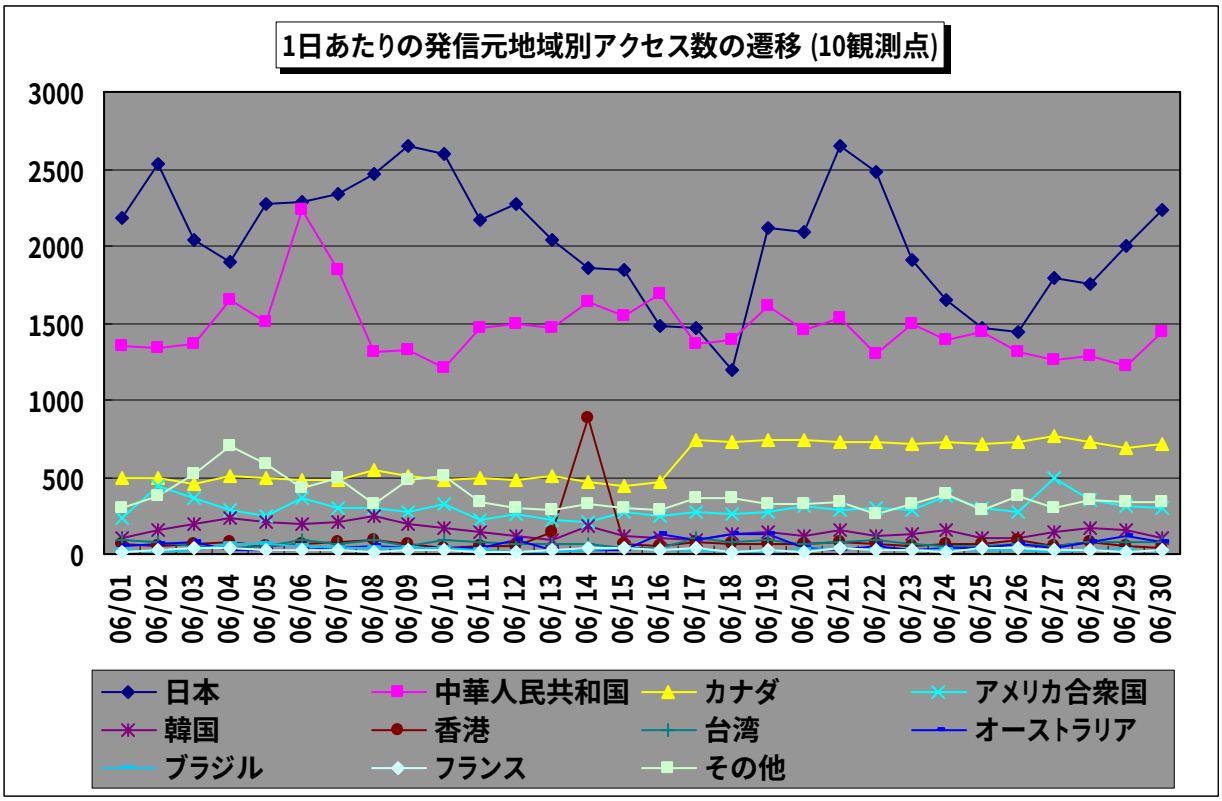
【図 2.3.1 2008 年 6 月の宛先(ポート種類)別アクセス数の比率】



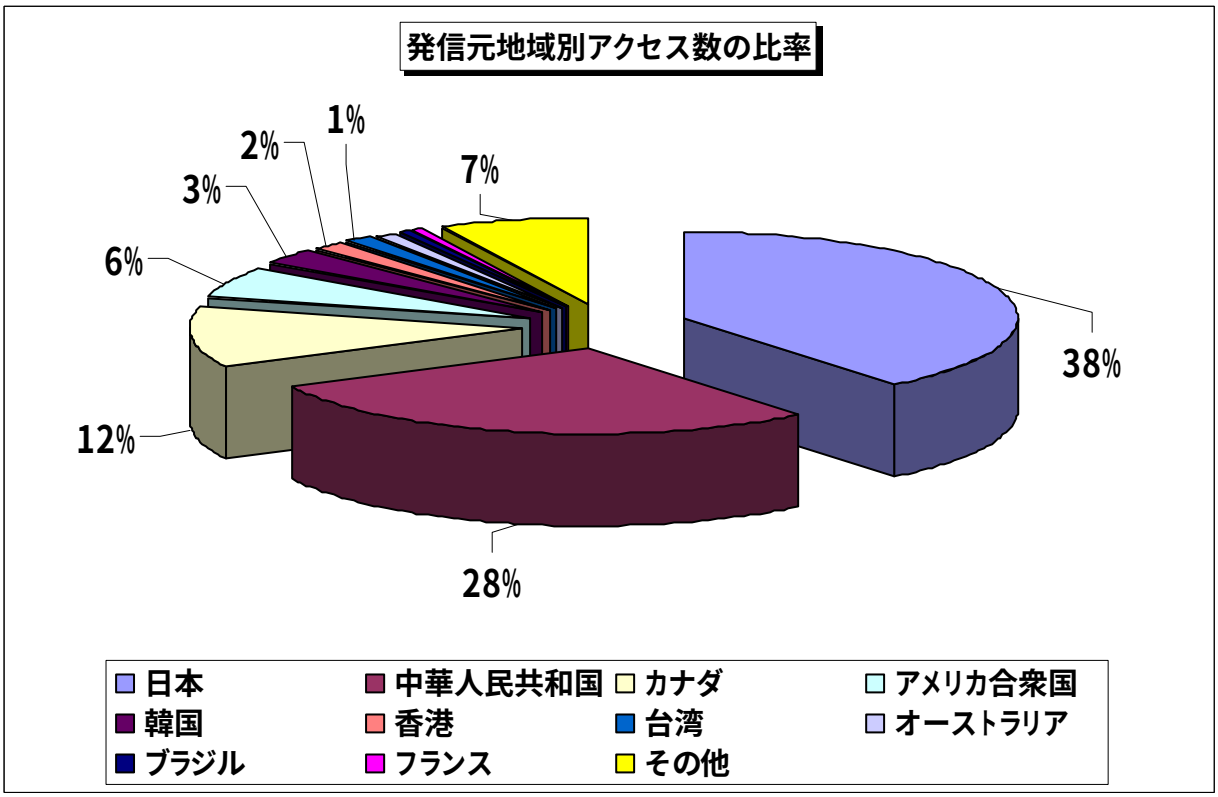
【図 2.3.2 2008 年 6 月の宛先(ポート種類)別発信元数の比率】

2.4 2008 年 6 月の発信元地域別アクセス状況

2008 年 6 月の一方的なアクセスの発信元地域別アクセス数の変化を図 2.4.1 に、発信元地域別アクセス数の比率を図 2.4.2 に示します。

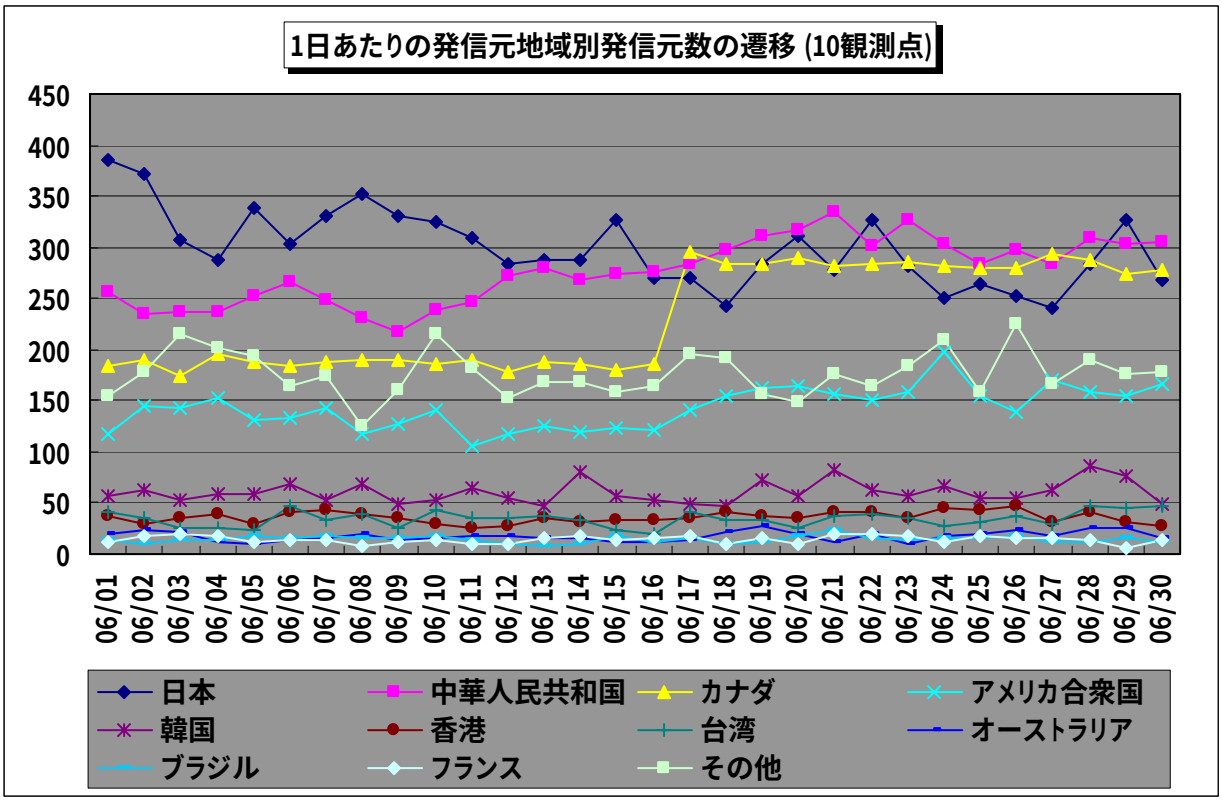


【図 2.4.1 2008 年 6 月の発信元地域別アクセス数の変化】

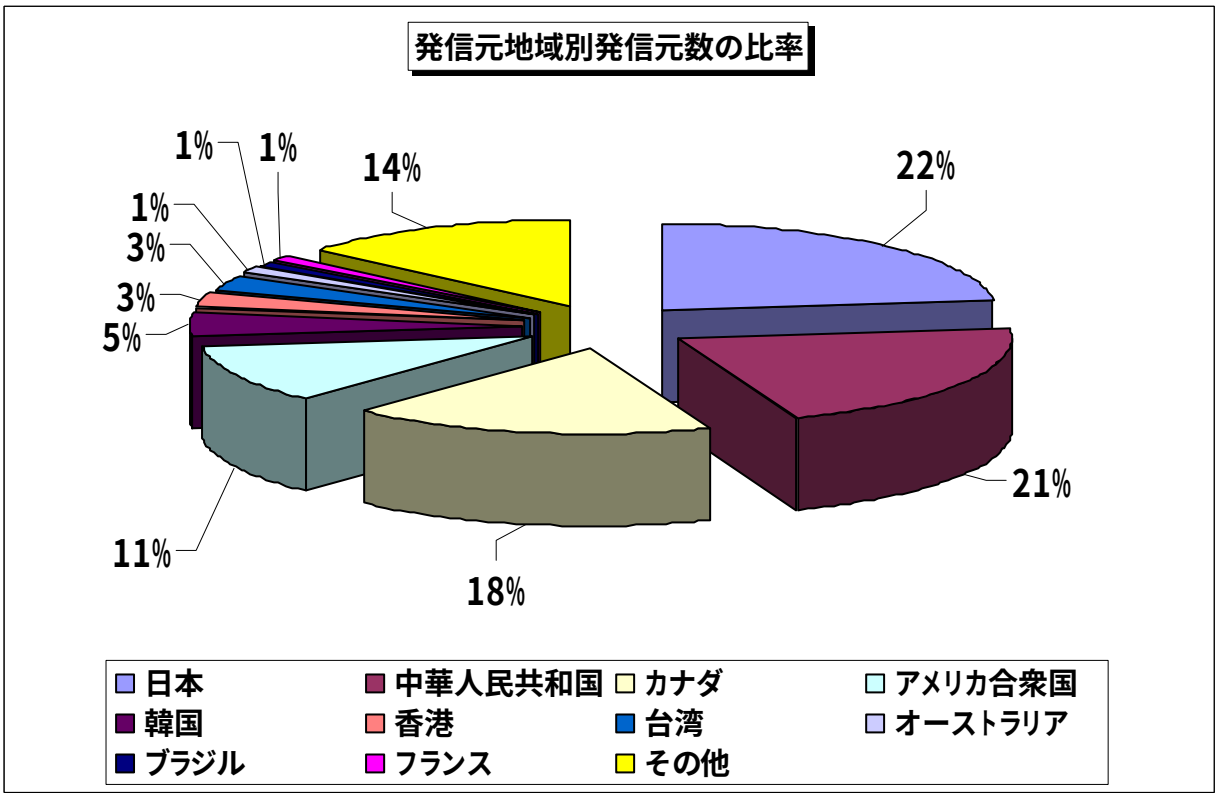


【図 2.4.2 2008 年 6 月の発信元地域別アクセス数の比率】

2008 年 6 月の一方的なアクセスの発信元地域別発信元数の変化を図 2.4.3 に、発信元地域別発信元数の比率を図 2.4.4 に示します。



【図 2.4.3 2008 年 6 月の発信元地域別発信元数の変化】

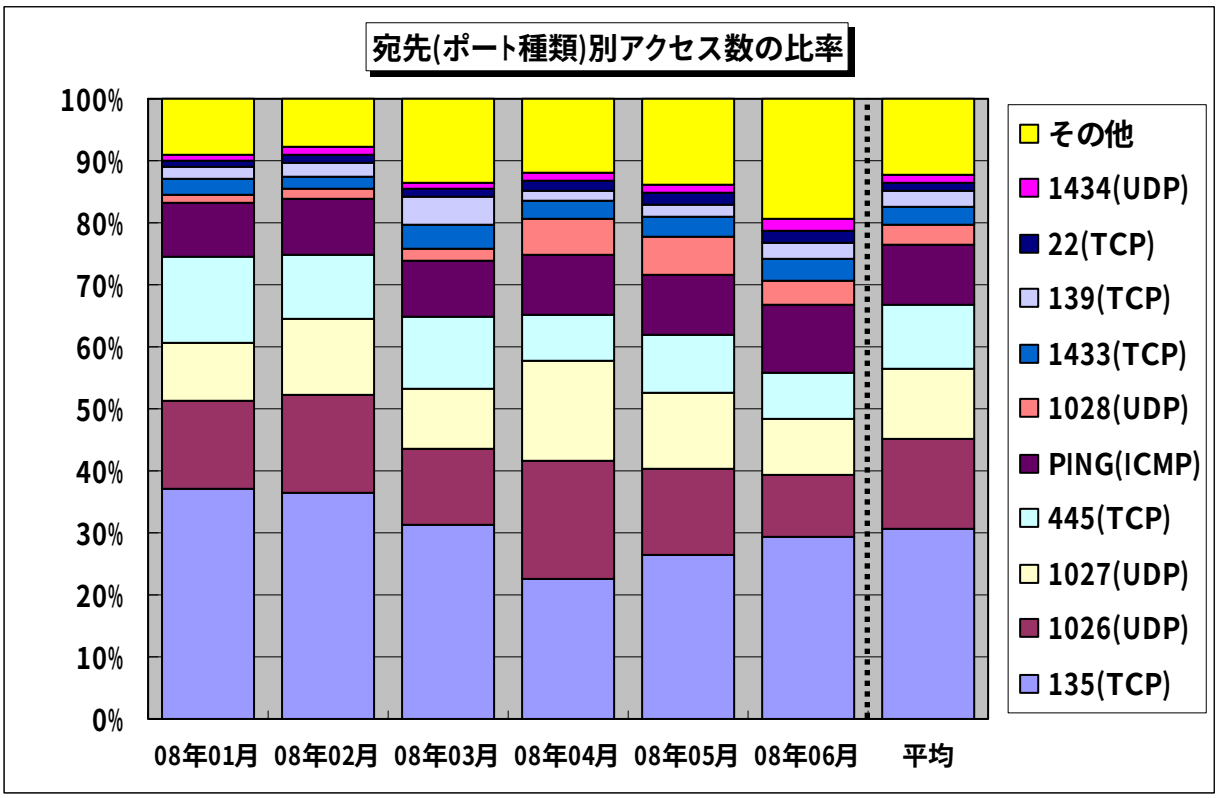


【図 2.4.4 2008 年 6 月の発信元地域別発信元数の比率】

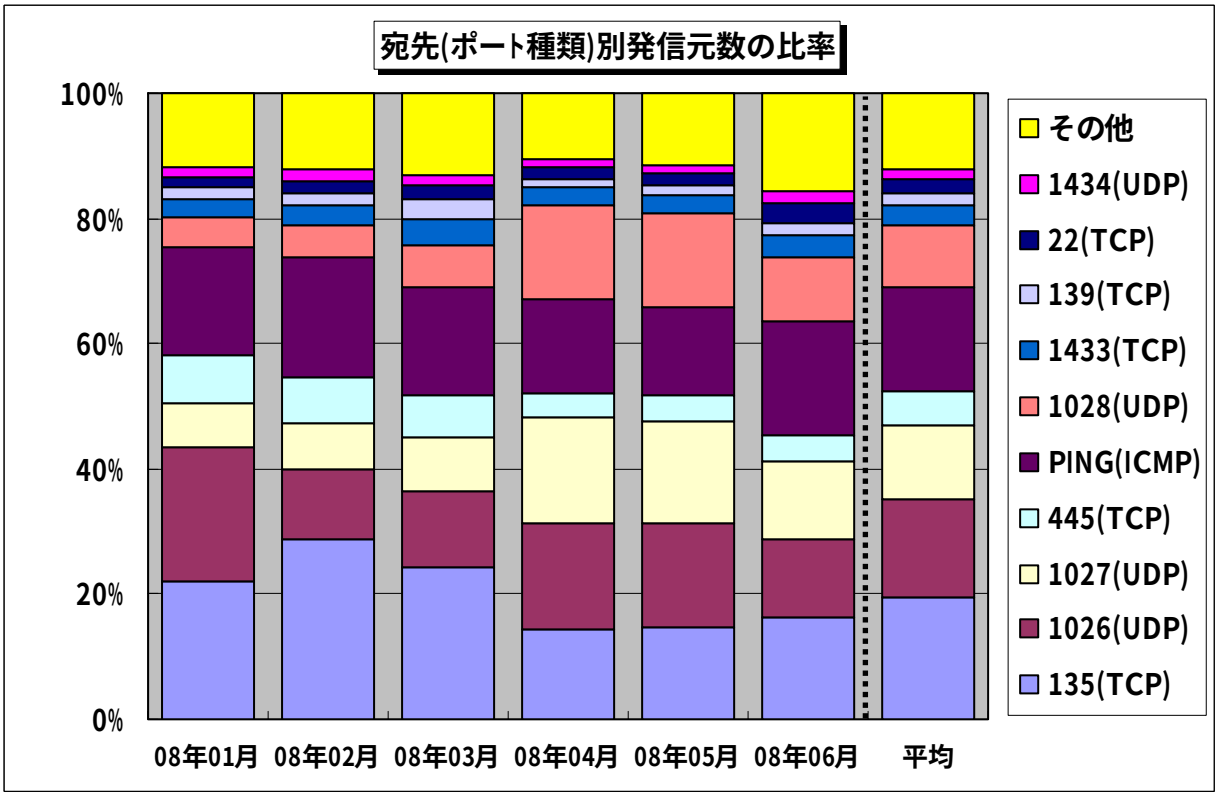
3．統計情報

3.1 2008 年 1 月～2008 年 6 月の宛先(ポート種類)別の比率

2008 年 1 月～2008 年 6 月の宛先(ポート種類)別アクセス数の比率を図 3.1.1 に、宛先(ポート種類)別発信元数の比率を図 3.1.2 に示します。



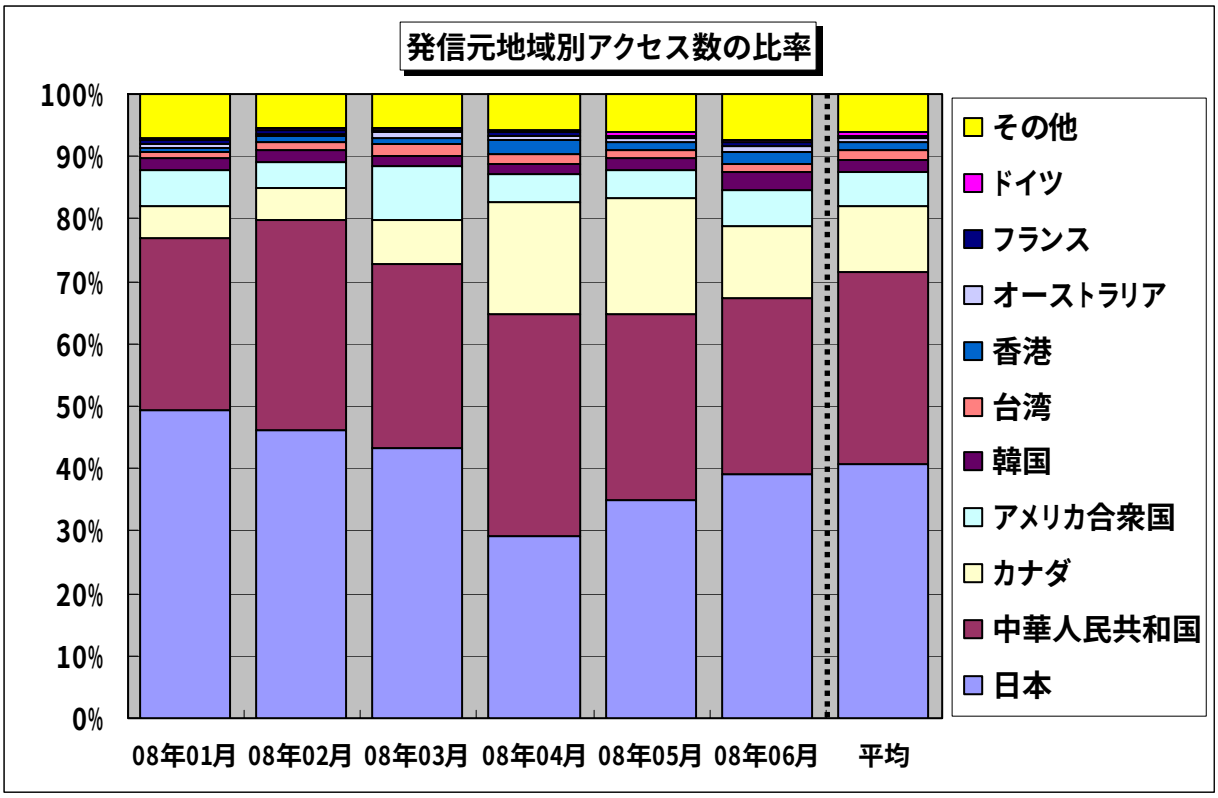
【図 3.1.1 2008 年 1 月～2008 年 6 月の宛先(ポート種類)別アクセス数の比率】



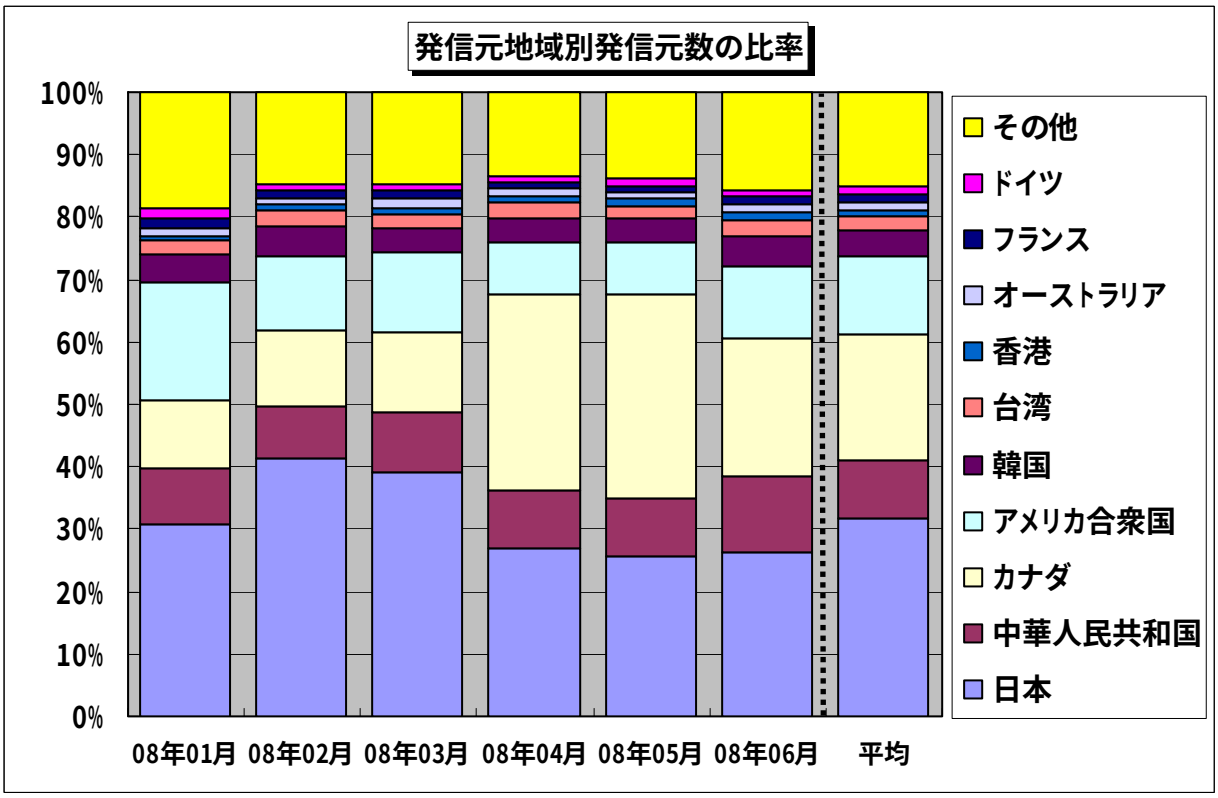
【図 3.1.2 2008 年 1 月～2008 年 6 月の宛先(ポート種類)別発信元数の比率】

3.2 2008 年 1 月～2008 年 6 月の発信元地域別の比率

2008 年 1 月～2008 年 6 月の発信元地域別アクセス数の比率を図 3.2.1 に、発信元地域別発信元数の比率を図 3.2.2 に示します。



【図 3.2.1 2008 年 1 月～2008 年 6 月の発信元地域別アクセス数の比率】



【図 3.2.2 2008 年 1 月～2008 年 6 月の発信元地域別発信元数の比率】

4．補足説明

以下に、2008 年 6 月にアクセス数の多かった宛先(ポート種類)の解説を行います。

ポート種類	解説
Ping(ICMP)	相手のコンピュータが動作中か調べる目的で使用されるが、不正アクセスの対象コンピュータを探す目的で、W32/Welchia などに利用されたことで有名
22(TCP)	パスワードクラッキング攻撃によるシステムへの侵入を目的とした、SSH（Secure Shell：通信路を暗号化することで安全性を高めたリモートからのコマンド実行ツール）を狙ったアクセスです
135(TCP)	Microsoft Windows Remote Procedure Call(RPC)のデフォルトポートであり、RPC に関する脆弱性(MS03-026)を狙った不正アクセスが有名(W32/MSBlaster など)
139(TCP)	保護のあまいファイル(ネットワーク)共有を狙った不正アクセスが有名ですが、一般的に Windows の脆弱性を狙ったアクセスである可能性が高いです
445(TCP)	保護のあまいファイル（ネットワーク）共有や Windows2000 特有の脆弱性を狙った不正アクセスが有名（W32/Sasser など）
1026(UDP)/1027(UDP)/1028(UDP)	Microsoft Windows Messenger service（MSN Messenger とは別物）を利用したポップアップ(スパム)メッセージの送信で有名
1433(TCP)	Microsoft SQL Sever の既定ポートであり、SQL Server が動作中のコンピュータを探す目的や、SQL Server の脆弱性を狙った不正アクセスなど
1434（UDP）	Microsoft SQL Sever の脆弱性を狙った不正アクセスなどが有名（W32/SQLSlammer など）
5900(TCP)	リモートアクセスツール RealVNC のぜい弱性を狙っていると思われるアクセスです

■お問い合わせ先
独立行政法人 情報処理推進機構 セキュリティセンター
大浦／望月／加賀谷
Tel:03-5978-7527 Fax:03-5978-7518
E-mail: isec-info@ipa.go.jp